Department of Homeland Security

Office of Inspector General

U.S. Customs and Border Protection
Privacy Stewardship

OIG-12-78

April 2012

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 30, 2012

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

This report addresses the U.S. Customs and Border Protection's plans and activities to instill a culture of privacy that protects sensitive personally identifiable information and ensures compliance with Federal privacy laws and regulations. This report is based on interviews with employees and officials of relevant agencies and subcomponents, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Charles K. Edwards
Acting Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
ICE	U.S. Immigration and Customs Enforcement
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information
TECS	formerly Treasury Enforcement Communications System
TSA	Transportation Security Administration
USCIS	U.S. Citizenship and Immigration Services

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

We performed an audit of U.S. Customs and Border Protection's (CBP) privacy stewardship. Our audit objectives were to determine whether CBP's plans and activities instill a culture of privacy that protects sensitive personally identifiable information and whether CBP ensures compliance with Federal privacy laws and regulations.

CBP has made limited progress toward instilling a culture of privacy that protects sensitive personally identifiable information. This is in part because it has not established a strong organizational approach to address privacy issues across the component. To strengthen its organizational approach to privacy, CBP needs to establish an Office of Privacy with adequate resources and staffing and hold Assistant Commissioners and Directors accountable for their employees' understanding of and compliance with their privacy responsibilities.

In addition, CBP needs to improve its compliance with Federal privacy laws and regulations. Specifically, it needs to develop a complete inventory of its personally identifiable information holdings, complete privacy threshold analyses for all systems, and develop accurate system of records notices for its systems. CBP also needs to ensure that privacy impact assessments are conducted for all personally identifiable information systems.

CBP also needs to implement stronger measures to protect employee Social Security numbers. Without a component-wide approach to minimizing the collection of employee Social Security numbers, privacy incidents involving these numbers will continue to occur.

Respondents to our privacy survey provided thousands of suggestions on how CBP can better instill a culture of privacy. We are making three recommendations to the Acting Commissioner of CBP.

Background

The *Privacy Act of 1974*, as amended (Privacy Act) imposes various requirements on agencies whenever they collect, use, maintain, or disseminate personally identifiable information (PII) in a system of records. The Department of Homeland Security (DHS) defines PII as any information that permits the identity of an individual to be inferred directly or indirectly, including any information that can be linked to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the United States, employee, or contractor to the Department. Federal laws, regulations, directives, and guidelines set the minimum standards for handling PII. Appendix C lists Federal privacy laws and policies related to CBP privacy stewardship.

CBP secures the Nation's borders, protects the public against terrorists, and facilitates the flow of legitimate international trade and travel. To accomplish CBP's mission, different groups of CBP employees may collect, use, maintain, or process PII on a daily basis, as shown in figure 1.

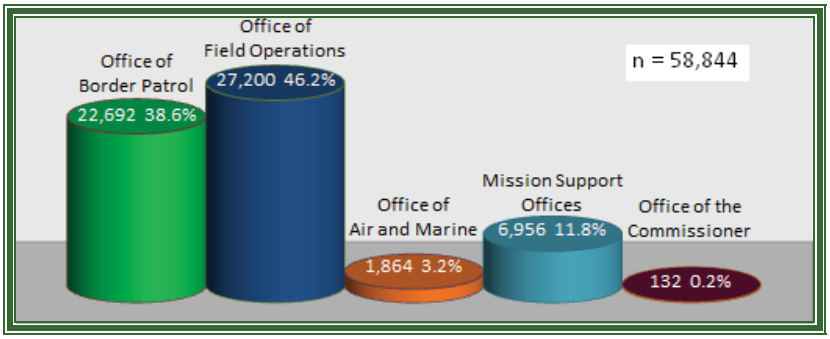

Figure 1. U.S. Customs and Border Protection Employee Groups

The Office of Border Patrol and the Office of Field Operations account for almost 85 percent of CBP's employees. These offices may handle a significant volume of PII. For example, more than 20,000 border agents collect, handle, share, or maintain PII to secure 6,900 miles of border with Canada and Mexico, as well as 95,000 miles of shoreline. In fiscal year 2010, more than 23,000 field officers and specialists at ports of entry collected, handled, shared, or maintained PII related to more than 350 million travelers, 105 million conveyances (cars, trucks, buses, trains, vessels, and aircraft), and 24 million truck, rail, and sea containers.

CBP employees use 46 information technology systems that maintain Social Security numbers, biometric data, and financial information. For example, one system stores more than 35

terabytes of PII[1] Figure 2 shows examples of PII that CBP collects from data owners and stores in different systems.

CBP System	From Whom Or What	What Personally Identifiable Information May Be Collected
TECS System: CBP Primary and Secondary Processing	Traveler	name, date of birth, address, gender, citizenship, Social Security number, phone number, occupation, photo, fingerprint ID number, driver's license data, vehicle information, dates and method of arrival/departure
Automated Targeting System	Traveler Conveyance Cargo	list of passengers and crew on flight, passenger name records that include name, address, flight, seat number, cargo destination, and account data
Automated Commercial System/ Automated Commercial Environment	Broker Carrier Importer Cargo	name, date of birth, address, gender, citizenship, driver license data, travel document data, destination, account data, electronic manifests
Advanced Passenger Information System/ Non-Immigrant Information System	Passenger Crew	name, date of birth, gender, citizenship, passport information, travel document type, U.S. address for foreign nationals, passenger name records, pilot license, country of issue for aircrew

Figure 2. Types of Personally Identifiable Information Collected by CBP

A component's culture of privacy reflects how well its executive leadership, managers, and employees understand, implement, and enforce a commitment to protect privacy. Privacy stewardship, or the promotion of an effective culture of privacy, leads to embedded shared attitudes, values, goals, and practices for complying with the requirements for proper handling of PII. A component privacy office can help enhance the culture of privacy by identifying privacy issues and working within the component to address them.

An effective culture of privacy supports ongoing risk assessment, assurance that appropriate safeguards are followed to protect individual PII and full sustainment of privacy compliance. Serious consequences to PII can result if CBP does not regularly assess and confirm whether PII is secure in its information technology systems. For example, a data breach of a major information technology system has been estimated to cost an average of $213 per record to resolve each privacy incident.[2] Given the significant volume and critical nature of the 1.2 million records containing traveler's identity information generated in CBP's TECS (formerly

[1] A terabyte is a unit of measurement for digital information that is equivalent to 1 trillion bytes. One terabyte is equivalent to the information stored in a large public library. Therefore, 35 terabytes are equivalent to 35 large public libraries.

[2] According to the Ponemon Institute 2010 Annual Study: *U.S. Cost of a Data Breach*, March 2011, data breaches cost an average of $213 per compromised record, which includes the costs of investigating the breach, preparing breach notifications, and providing credit monitoring to affected individuals.

the Treasury Enforcement Communications System) in a single day, a data breach could cost $255.6 million. By complying with privacy requirements, including risk assessment and mitigation, CBP would be able to perform its mission while minimizing negative impact on individual privacy.

On June 5, 2009, the DHS Deputy Secretary issued the DHS Memorandum *Designation of Component Privacy Officers* (DHS Designation Memorandum), directing 10 components, including CBP, to designate senior-level Federal employees as their full-time Privacy Officers. CBP selected a Branch Chief under the Office of International Trade as the Privacy Officer, but decided to retain his existing organizational placement. CBP responded to the DHS Deputy Secretary that this placement would "comply, substantially, with…[the DHS Designation Memorandum]…as well as with the constraints imposed upon CBP by both the *Homeland Security Act of 2002* and the *Security and Accountability for Every Port Act of 2006* (SAFE Port Act)."[3] The selected Privacy Officer continues to perform the full-time responsibilities as one of the many Branch Chiefs in the Office of International Trade.

The DHS Designation Memorandum requires the component Privacy Officers to report to the head of the component. When acting as the CBP Privacy Officer, he reports through the Assistant Commissioner of the Office of International Trade to the Commissioner. Figure 3 illustrates the organizational placement of the two distinct positional responsibilities and respective information flow, one as the Privacy Officer (blue box and dotted line to show informal information flow) and another as the Branch Chief (green box and solid line to show his formal reporting line).

[3] The SAFE Port Act mandated compliance with Section 412(b) of the Homeland Security Act that required legacy U.S. Customs revenue functions to continue under the newly established DHS, to include the specific allocation of staff in trade facilitation. Therefore, the staff of the Office of International Trade inherited the mandatory staffing requirements because they facilitate CBP's compliance with the SAFE Port Act.

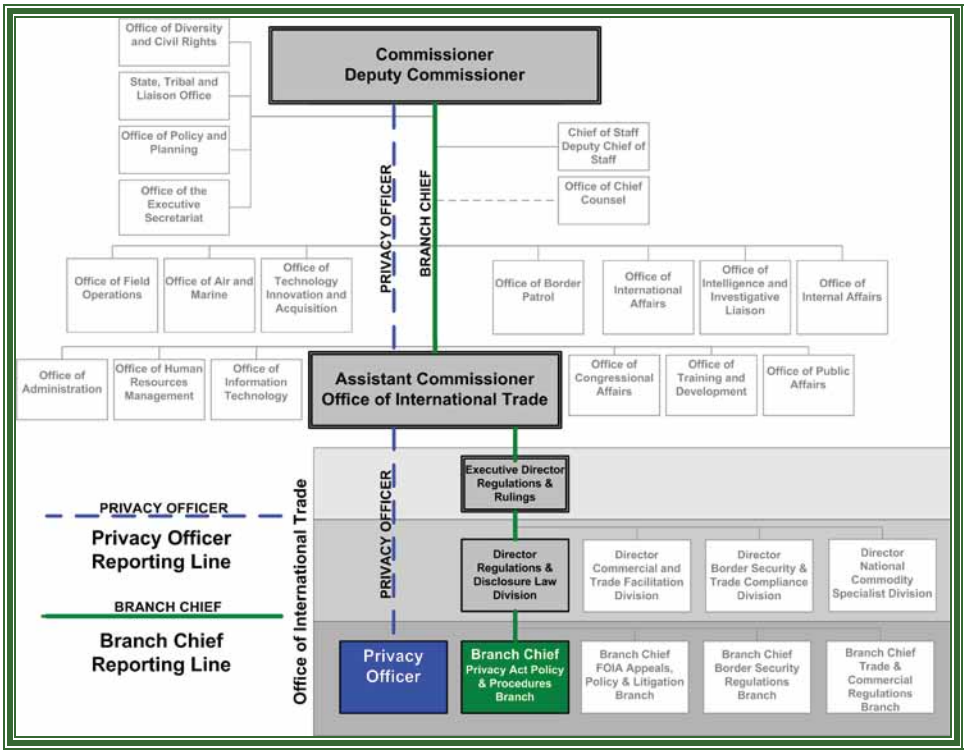

Figure 3. Privacy Officer Placement and Reporting

Results of Audit

CBP Needs To Strengthen Its Organizational Approach to Privacy

CBP has made limited progress toward instilling a culture of privacy. This is in part because it has not established a strong organizational approach to address privacy issues across the component. CBP designated one of its senior officials as its Privacy Officer in July 2009. As indicated in figure 3, his assignment is collateral with his responsibilities as Branch Chief, limiting his ability to address fully the wide array of duties described in the DHS Designation Memorandum. (See appendix D for a complete list of duties required of component Privacy Officers.)

For example, CBP has not issued a privacy directive outlining an organizational approach to ensure proper handling of PII and a strategic vision on privacy matters. Such a directive would formally hold Assistant Commissioners and Directors accountable for their employees' understanding of and compliance with all Federal privacy laws and regulations. The strategic vision would support managers and staff in working closely with the Privacy Officer and including him in all management strategy meetings and operational planning that could affect privacy. The Privacy Officer is best situated to identify the privacy issues related to CBP's mission and work with managers on how best to

implement DHS privacy policies into their specific operations. By implementing a privacy directive, CBP would improve the presence and effectiveness of the CBP Privacy Officer and the extent to which he can perform essential duties, such as the following:

- Monitoring the component's compliance with all Federal privacy laws and regulations; implementing corrective, remedial, and preventive actions; and, notifying the DHS Privacy Office of privacy issues or noncompliance when necessary;
- Assisting in drafting and reviewing privacy threshold analyses, privacy impact assessments, and system of records notices, as well as any associated privacy compliance documentation; and,
- Implementing and monitoring privacy safeguards, including training, for employees and contractors.

Also according to the DHS Designation Memorandum, components are to provide their Privacy Officers with adequate support and resources. CBP, however, has provided staff members to manage on a part-time basis a privacy program for the 58,000 employees who handle PII. Other DHS components—including the Federal Emergency Management Agency (FEMA), United States Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), and United States Citizenship and Immigration Services (USCIS)—support their respective privacy programs with anywhere from 3 to 13 full-time staff. Figure 4 shows the components that have issued privacy directives or policies to hold formally their managers accountable for their operations' compliance with privacy requirements.

Component	Est. # Employees Handling Personally Identifiable Information	Formally Established Management Accountability	# Staff Provided for Privacy Office
CBP	58,000	No	11 (collateral duty)
FEMA	7,000	Yes	8
ICE	13,000	Yes	5
TSA	20,000	Yes	3
USCIS	18,000	Yes	13

Figure 4. Comparable DHS Component Privacy Offices

We conducted a survey of CBP's culture of privacy to assess privacy knowledge and obtain responses on three questions regarding privacy risks and integrating privacy into daily operations. (See appendix E for the survey methodology, details, and results.) More than 650 responses addressed the need for CBP to provide a shared strategic vision on privacy matters. Almost 800 responses indicated that managers can improve

privacy stewardship. CBP officials whom we interviewed said that more resources and management accountability are needed to ensure that CBP has an effective privacy program. As discussed in the following sections, CBP continues to face challenges in ensuring the protection of PII across the component.

CBP Needs To Improve Compliance With Privacy Requirements

CBP needs to improve its overall compliance with Federal privacy laws and regulations. Specifically, CBP needs to develop a complete inventory of all of its holdings of PII. In addition, CBP needs to conduct privacy threshold analyses to identify all systems that affect privacy.[4] Further, CBP needs to ensure that published system of records notices accurately reflect employee practices in handling the public's PII. Finally, CBP needs to perform privacy impact assessments for its systems.

Inventory of Holdings for Personally Identifiable Information Is Not Complete

CBP's inventory of its holdings for PII is not complete. Office of Management and Budget (OMB) M-07-16 requires agencies to review their holdings of all PII and ensure that they are accurate, relevant, timely, and complete. Holdings for PII include systems, programs, and records that are privacy sensitive.

CBP cannot confirm the collection, location, and status of all of its PII. For its inventory of holdings for PII, CBP has relied on an electronic system, Trusted Agent Federal Information Security Management Act (Trusted Agent). Trusted Agent tracks only general support information technology systems and major applications.[5] General support information technology systems and major applications do not include other subsystems, modules, applications, programs, or records that collect, use, disseminate, or maintain personally identifiable information. Therefore, Trusted Agent does not contain a complete inventory of holdings for personally identifiable information.

[4] For this report, we use "system" to refer to a system of records as well as information technology systems (e.g., subsystems, modules, applications), programs, rule-making, or technology that may be sensitive to privacy. A system of records may be paper-based or electronic. A system of records is a group of any records about an individual under agency control from which information is retrieved by that individual's name, identifying number, symbol, or other identifying particular assigned to the individual.

[5] Trusted Agent is a software application that the DHS Office of the Chief Information Officer uses to comply with the *Federal Information Security Management Act of 2002*. DHS uses Trusted Agent to track major systems, including those that affect privacy. Components retain certain privacy compliance documentation along with security documentation in Trusted Agent.

CBP's information technology staff is responsible for tracking and updating documentation for the 101 major information technology systems in Trusted Agent. Figure 5 shows how CBP has categorized the privacy status of these information technology systems.

Number of systems in inventory of personally identifiable information	47
Number of information technology systems without personally identifiable information in inventory	54
Total number of systems in Trusted Agent inventory	101

Figure 5. Trusted Agent Inventory
Source: DHS Privacy Office, Trusted Agent, and CBP records, as of July 15, 2011.

In addition, CBP has not accounted for all of its systems. Through analysis of the Trusted Agent inventory, reports from the DHS Privacy Office, and CBP's Intranet website, as well as information gathered from interviews, we determined that there are at least 48 potential systems that are in neither Trusted Agent nor the CBP Privacy Officer's inventory list. Examples include systems to track cargo, intellectual property rights, passenger screening, and private aircraft. (See appendix F for information on CBP's systems.) Because it has not identified all of its systems, CBP cannot ensure that effective privacy protections and mitigation of privacy risks for its systems, programs, and records have been implemented.

Privacy Threshold Analyses Not Performed

CBP has not conducted privacy threshold analyses for all of its systems. The DHS Privacy Office requires component program managers to submit a privacy threshold analysis every three years, when significantly changing existing systems, or when proposing new systems of records. The privacy threshold analysis is used to identify the systems that affect privacy.

More than 70 percent (71 of 101) of CBP's systems need privacy threshold analyses. Specifically, 32.7 percent (33 of 101) of systems in Trusted Agent still require privacy threshold analyses, and 37.6 percent (38 of 101) of systems have expired privacy threshold analyses that need to be updated. Only 29.7 percent (30 of 101) of CBP privacy threshold analyses are current. In addition, there are 48 potential systems that need privacy threshold analyses. (See appendix F for status.) Once CBP submits a privacy threshold analysis, the DHS Privacy Office determines whether

(a) the activity involves PII, (b) a privacy impact assessment is required, and (c) an existing or new system of records notice is required for a collection of PII.

System of Records Notices

CBP has not developed system of records notices for all of its systems, as required by the Privacy Act. Specifically, 22.7 percent (10 of 44) of CBP's systems do not have system of records notices. The Privacy Act requires Federal agencies to issue a notice for all systems of records under their control that collect personally identifiable information and from which information is retrieved by a unique identifier. The system of records notices provide to the public the rights and procedures for accessing and correcting personally identifiable information maintained by an agency on an individual.[6]

In addition, all of CBP's published system of records notices for the remaining 34 (of 44) systems contain inconsistent information regarding the 26 types of records that they describe. For example, some records are being disposed of before the dates specified in their respective system of records notices. Other records are being held longer than the times identified in their respective system of records notices. According to the Privacy Act, information in the system of records notices must accurately describe how Government employees are handling the public's PII. (See appendix G for additional information on inconsistencies between CBP system of records notices and internal guidance.)

Privacy Impact Assessments Are Not Performed

CBP has not conducted privacy impact assessments for all of its systems. The *E-Government Act of 2002* requires agencies to conduct privacy impact assessments for all new or substantially changed information systems that collect, maintain, or disseminate PII. The privacy impact assessment process is a decision-making tool that requires pertinent information for analysis to ensure that privacy protections are incorporated during the development and operation of systems and programs that affect personally identifiable information.

[6] System of Records Notices are published in the *Federal Register* to inform the public about what personally identifiable information is being collected, why it is being collected, how long it is being retained, and how it will be used, shared, accessed, and corrected. The *Federal Register* is the official daily publication for rules, proposed rules, and notices of Federal agencies and organizations, as well as executive orders and other presidential documents, and is published by the Office of the Federal Register, National Archives and Records Administration.

Although the DHS Privacy Office required privacy impact assessments for 31 of CBP's systems, 58.1 percent (18 of 31) of these systems still do not have them, as indicated in figure 6. Only 41.9 percent (13 of 31) of the systems have approved privacy impact assessments that are posted on the DHS Privacy Office website. In addition, as identified in the section regarding privacy threshold analyses, 48 systems may need privacy impact assessments, as well.

Number of systems with completed privacy impact assessments	13
Number of systems without privacy impact assessments	18
Total number of systems that require privacy impact assessments	31

Figure 6. Status of Privacy Impact Assessments
Source: DHS Privacy Office, Trusted Agent, and CBP records and interviews, as of July 15, 2011.

Stronger Measures Needed To Protect CBP Employee Social Security Numbers

CBP has not taken appropriate measures to protect its employees' Social Security numbers. In June 2007, the Office of Personnel Management issued guidance and instructions for agencies to eliminate the unnecessary use of employee numbers as identifiers and to strengthen the protection of employee Social Security numbers from theft or loss. However, CBP has not implemented component-wide measures to eliminate the unnecessary collection of employee Social Security numbers on electronic and paper forms, nor has it employed effectively alternative identifiers. Without implementing such measures, CBP increases the risk that employee Social Security numbers will be lost or stolen.

Unprotected Social Security Numbers on Electronic and Paper Forms

CBP has not implemented sufficient measures to protect Social Security numbers in information systems or on paper forms. DHS Privacy Policy Guidance Memorandum 2007-02 *Regarding the Use of Social Security Numbers at DHS* allows programs to collect, use, maintain, and disseminate Social Security numbers as unique identifiers only when required by statute or regulation. Absent a legal requirement, DHS programs are to create their own unique identifiers to identify or link information about individuals.

Although CBP posted DHS Memorandum 2007-02 on its Intranet site for the Training Records And Enrollment Network, it

maintains training records for more than 58,000 employees and continues to collect, store, and track employee Social Security numbers for course enrollments. According to CBP officials, the current training network was designed to use employees' Social Security numbers as unique identifiers. To correct this oversight and improve the functionality of the system, a new training network is being developed that does not use employees' Social Security numbers as unique identifiers.

In addition, TECS is a system that supports enforcement and inspection operations by tracking and processing data on suspect individuals, businesses, vehicles, aircraft, and vessels entering the United States by air, land, or sea. TECS data are maintained and updated by more than 58,000 CBP employees, as well as another 12,000 employees in more than 20 Federal agencies. TECS maintains a history or log of employee user activities. When we viewed various logs on TECS screens, we were able to see the names and Social Security numbers of the employees who collected, accessed, and maintained TECS information.[7] The same screens with employee Social Security numbers can be viewed by TECS users at ports of entry, bridges, land borders, and in field offices and vehicles. CBP is currently modernizing TECS. As part of this effort, CBP will implement new procedures to protect employee Social Security numbers.

Finally, CBP has not minimized the collection of employee Social Security numbers on all of its administrative paper forms. Most of these forms require only names, partial Social Security numbers, alternative identifiers, or Social Security numbers for financial and security reasons. However, we also identified forms that require employees to provide their complete Social Security numbers without identifying any legal authority for them. For example, we found forms requiring employees' complete Social Security numbers regarding canines, personal clothing, and equipment.

Insufficient Use of Alternative Identifiers

OMB M-07-16 states that agencies should explore alternatives to the use of Social Security numbers as personal identifiers for Federal employees. Since 2007, CBP has been issuing "HASH-IDs" to comply with OMB guidance, but has not required their use to replace Social Security numbers.[8] According to CBP officials, HASH-IDs cannot be required component-wide because they are

[7] TECS also contains the public's Social Security numbers. Additional information is provided about TECS on pp. 3–4 of this report.
[8] A HASH-ID is a unique identifier for each CBP employee.

not supported by all information technology systems, such as the Training Records And Enrollment Network. By continuing to use employee Social Security numbers, CBP places them at an unnecessary risk of disclosure.

Privacy Incidents Concerning Social Security Numbers

Without a strong approach to minimizing the collection of employee Social Security numbers and implementing effective measures to protect them, privacy incidents involving employees' Social Security numbers continue to occur. For example, as reported by CBP to the DHS Security Operations Center during a 2-year period (2009 to 2010)—

- An e-mail containing Social Security numbers for 75 individuals was sent to 13 other employees who had no need to know this information.
- A personal digital camera was used to take a picture of a computer monitor that displayed the names, Social Security numbers, and dates of birth of 33 airport employees.
- An e-mail containing the Social Security number of an employee was sent to two FEMA employees who were not intended to receive the e-mail.
- Three unencrypted DVDs containing Social Security numbers were sent to a new duty location using a commercial delivery service.

In addition, respondent comments to our culture of privacy survey identified two common situations that we confirmed at CBP work locations in which employee Social Security numbers had been placed at risk unnecessarily. First, some supervisors and employees have left paper copies of forms with employee Social Security numbers in unattended areas where someone from the public would have access, such as on the front desk of a reception area. Second, some supervisors and staff have verbally disclosed employee Social Security numbers in open areas of offices within earshot of people who would normally not have access to or a "need to know" PII. Without implementing measures to minimize and protect the use of employees' Social Security numbers, CBP is increasing the risk that employee PII will be lost or stolen.

Survey Respondents Suggest Improvements to Privacy Safeguards

The Privacy Act requires that agencies implement administrative, physical, and technical safeguards to ensure the security and confidentiality of records. In addition, these safeguards should protect against any anticipated threats or hazards that could result in substantial harm to individuals from whom information is collected. More than 40 percent (2,907 of 7,229) of written comments by respondents to CBP's culture of privacy survey related to improving privacy safeguards.

Employees provided 817 comments or suggestions concerning privacy training. These comments included the need for CBP to—

- Provide in-person, instructor-led training at field sites (346);
- Provide more frequent training (232);
- Incorporate on-the-job and real-world examples related to different programs and operations (85);
- Improve training of contractors who work in areas where PII is handled (74);
- Develop specialized privacy training for particular groups, such as new employees, supervisors, and executive managers (49); and
- Simplify the presentation and concepts during privacy training, so they can be applied more easily to daily operations (31).

Employees also provided 552 comments or suggestions on improving other administrative safeguards. These comments included the need for CBP to—

- Consolidate forms and databases to reduce duplication of PII (381);
- Enforce existing DHS policies on protecting PII, such as conducting internal audits to determine compliance with required safeguards on the job (155); and
- Conduct thorough background checks of employees and contractors who are responsible for handling PII (16).

In addition, employees provided 734 comments or suggestions on improving physical safeguards. These comments included the need for CBP to—

- Adjust layout of work areas to improve the protection of PII (211);
- Supply drawers or bins to secure PII (192);
- Provide locks on cabinets and containers to secure PII (133);

- Provide privacy screens or adjust the placement of monitors to prevent onlookers from seeing PII (93);
- Address general issues related to physical safeguards (78); and
- Improve physical barriers to prevent unauthorized persons from accessing government computers (27).

Finally, employees provided 804 comments or suggestions on improving technical safeguards. These comments included the need for CBP to—

- Enforce consistent application of password protection and encryption (481);
- Establish limitations on access to databases (142);
- Implement technical solutions to prevent unauthorized access to data on personal electronic devices and removable storage media (88);
- Address general issues related to technical safeguards (74); and
- Consider automated alerts and pop-ups to prompt users to protect PII (19).

Recommendations

We recommend that the Acting Commissioner of CBP:

Recommendation #1: Establish an Office of Privacy with adequate resources and staffing to ensure that CBP is able to fulfill its privacy responsibilities.

Recommendation #2: Issue a directive that holds Assistant Commissioners and Directors accountable for their employees' understanding of and compliance with their privacy responsibilities.

Recommendation #3: Implement stronger measures to protect employee Social Security numbers and minimize their use.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Assistant Commissioner of CBP's Office of Internal Affairs. A copy of the comments is in appendix B.

CBP concurred with recommendation #1. CBP's Acting Commissioner issued a memorandum entitled "Privacy Compliance and U.S. Customs and Border Protection," dated February 10, 2012. CBP indicated that it: (a) recognizes the expansion of its privacy role from that previously defined in the Deputy Secretary's

Memorandum, dated June 9, 2009, to include the review of information sharing activities as part of its privacy compliance role; (b) identifies its Privacy Office and associated staff as the attorney staff that has been assigned to the Office of International Trade since March 2003; and, (c) confirms that the identified staff positions remain assigned to the Office of International Trade to meet the Homeland Security Act of 2002 and the SAFE Ports Act of 2006. We consider recommendation #1 open and unresolved, pending our review of documentation regarding the allocation of adequate resources and staffing to ensure that CBP is able to fulfill its privacy responsibilities.

CBP concurred with recommendation #2. CBP's Acting Commissioner issued a memorandum to all Assistant Commissioners, the Chief of the Border Patrol, Chief Counsel, and all Executive Directors, entitled "Privacy Compliance and U.S. Customs and Border Protection," dated February 10, 2012, which disseminates the DHS Privacy Policy and Compliance Directive and Instructions, dated July 2011, for departmental guidance on privacy compliance. CBP indicated that both documents expand the privacy mission to include a role in reviewing information sharing activities. We consider recommendation #2 open and unresolved, pending our review of documentation that establishes accountability of Assistant Commissioners and Directors for their employees' understanding of and compliance with their privacy responsibilities.

CBP concurred with recommendation #3. CBP indicated that it has started implementation of a multi-year TECS Modernization Plan for the removal of Social Security numbers as user identification and a general visible identifier for TECS users and records owners. According to CBP, charges started with web applications for 30 internal CBP users in November 2011 and will continue with 12 external DHS users scheduled for March 2012. CBP indicates that TECS Modernization plans include functionality to remove the use of supervisor Social Security numbers from approval functions, affecting 8,000 users by March 2013. We consider recommendation #3 open and unresolved, pending our review of documentation regarding implementation of stronger measures to protect employee Social Security numbers and minimize their use.

Our objectives were to determine whether CBP has plans and activities that instill a culture of privacy that protects sensitive personally identifiable information and ensure compliance with Federal privacy laws and regulations. As background for this audit, we reviewed Federal laws and guidance related to CBP's responsibilities for privacy protections. We interviewed officials from the DHS Privacy Office on component privacy reporting. We reviewed testimonies, documentation, and reports related to CBP's privacy, information technology security, and program management.

In addition to interviewing CBP's Privacy Officer, we interviewed 60 program managers, officers, and information system security professionals at CBP headquarters and field sites. We e-mailed a survey to CBP employees to obtain their recommendations for improving their understanding of privacy and for an indication of their privacy knowledge. We received 7,229 individual comments on privacy risks, integrating privacy in daily operations, and challenges in CBP privacy stewardship. (See appendix E for details.)

We reviewed the privacy-related duties and activities performed by the CBP Privacy Officer, Records Officer, Training Office, and field personnel. We analyzed training programs and their content, as well as guidance on information technology and records management to determine whether they met the requirements of Federal privacy and security laws and regulations. We reviewed privacy threshold analyses, privacy impact assessments, and system of records notices for 47 systems identified in Trusted Agent that contain personally identifiable information and identified additional systems.

Our analysis is based on direct observation, review of applicable documentation, and interviews. We conducted this performance audit between April and November 2011 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, at (202) 254-4041 and Marj Leaming, Director, System Privacy Division, at (202) 254-4172. Major OIG contributors to the audit are identified in appendix I.

Appendix B
Management Comments to the Draft Report

1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and Border Protection

March 13, 2012

Charles K. Edwards
Acting Inspector General
Department of Homeland Security
245 Murray Drive, SW, Building 410
Washington, DC 20528

Re: The Office of Inspector General's Draft Report Entitled, "United States Customs and Border Protection Privacy Stewardship - For Official Use Only"

Dear Mr. Edwards:

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG's) draft report entitled "United States Customs and Border Protection Privacy Stewardship - For Official Use Only," (project no. OIG-11-016-ITA-CBP). U.S. Customs and Border Protection (CBP) appreciates the OIG's work in planning and conducting its review and issuing this report.

While CBP's Office of International Trade (OT) recognizes the vast scope of the task before the OIG in undertaking a full audit of all CBP, the audit does not provide a complete understanding of certain major information technology (IT) systems such as TECS. Authorized CBP employees use TECS and its various sub-systems and modules to fulfill numerous border security mission responsibilities. In the draft report the OIG, identifies TECS for its vast holdings of personally identifiable information (PII), and its legacy reliance upon the employee social security number (SSN) as a user identification (ID); however, the audit does not note that in over twenty years of service collecting information pertaining to all persons lawfully, and in some cases unlawfully, crossing the border, TECS has never had a major data breach as described in the example on pages three and four of the draft report.

CBP believes that the culture of privacy instilled through the mandatory requirement that each TECS user pass the TECS Privacy Awareness Course on an annual basis (39,301 users passed the test in FY 2011) contributes strongly to the enviable record TECS has established with respect to safeguarding its information holdings. Furthermore, this culture of privacy from TECS permeates not only the user communities of other CBP IT systems that rely upon passing the TECS privacy course to grant system access, but also creates a common bond of understanding with

respect to privacy and information sharing concepts. CBP has a strong culture of privacy that cannot simply be defined by the careful, deliberate, and cautious upgrade of TECS functionality.

Similarly, the Chart in Appendix F, starting on page 26, notes many PII holdings belonging to CBP, but does not adequately recognize the connections or coverage of these holdings in the privacy compliance documents pertaining to their larger IT systems. The discussion of the chart in the report implies that the holdings are not covered and exist as untracked or are not inventoried by CBP. Again, TECS serves as an example in that fifteen separate entries (out of the 49 listed in Appendix F) are identifiable to TECS and covered by the TECS privacy compliance. CBP draws attention to these representations so that the full scope of TECS compliance and risks can be known. Enclosed to this letter are CBP's technical comments which detail CBP's main concerns regarding the accuracy of system representations and PII holdings in Appendix F.

The report makes three recommendations for CBP. A summary of CBP actions and corrective plans to address the recommendations is provided below:

Recommendation #1: Establish an Office of Privacy with adequate resources and staffing to ensure that CBP is able to fulfill its privacy responsibilities.

CBP Response: Concur. CBP notes that certain staffing requirements of the Homeland Security Act of 2002 and the SAFE Ports Act of 2006, mandate that the staff and positions which have ensured CBP's privacy compliance since CBP was stood up in March 2003, remain identified to the attorney staff currently assigned to OT.

On February 10, 2012, the Acting Commissioner, CBP, issued a memorandum entitled "Privacy Compliance and U.S. Customs and Border Protection" to all Assistant Commissioners, the Chief of the Border Patrol, Chief Counsel, and all Executive Directors (see enclosed). The Acting Commissioner's Memorandum also disseminates the Privacy Policy and Compliance Directive and implementing Instructions issued by DHS in July 2011, during the pendency of the subject audit. These documents are noteworthy as they both provide departmental guidance with respect to privacy compliance and the role of privacy across the DHS enterprise, and clearly expand the privacy mission to include a role in reviewing information sharing activities. This expansion of the role defined in the June 9, 2009, memorandum from the Deputy Secretary clearly establishes the precedent for the full scope of the Acting Commissioner's Memorandum, and his charge to CBP. CBP believes that through the enclosed memorandum by its Acting Commissioner it has identified its Privacy Office and associated staff.

Accordingly, CBP respectfully requests closure of this recommendation.

Recommendation #2: Issue a directive that holds Assistant Commissioners and Directors accountable for their employees' understanding of and compliance with privacy responsibilities.

CBP Response: Concur. On February 10, 2012, the Acting Commissioner, CBP, issued a memorandum entitled "Privacy Compliance and U.S. Customs and Border Protection" to all Assistant Commissioners, the Chief of the Border Patrol, Chief Counsel, and all Executive Directors (see enclosed). The thrust of the memorandum emphasized the importance of privacy compliance throughout CBP not only in how CBP collects and maintains information obtained from the public, but also with respect to how CBP shares that information with its various federal, state, local, and foreign partners in fulfillment of its twin law enforcement and trade facilitation missions. CBP has enclosed to this letter a copy of Acting Commissioner's memorandum and the Privacy Compliance and Information Sharing process workflows that it disseminated to affirm a consistent practice and role for privacy in these two aspects of the CBP mission. The Acting Commissioner's Memorandum also disseminates the Privacy Policy and Compliance Directive and implementing Instructions issued by DHS in July 2011, during the pendency of the subject audit. These documents are noteworthy as they both provide departmental guidance with respect to privacy compliance and the role of privacy across the DHS enterprise, and clearly expand the privacy mission to include a role in reviewing information sharing activities.

Accordingly, CBP respectfully requests closure of this recommendation.

Recommendation #3: Implement stronger measures to protect employee Social Security numbers and minimize their use.

CBP Response: Concur. CBP concurs with this recommendation and notes that as part of its multi-year TECS Modernization Plan it has begun to implement IT solutions to remove the use of the SSN as a user ID and more generally as a visible identifier for TECS users and record owners. As part of the TECS modernization plan, a proof of concept for the TECS web applications was migrated to production for 30 TECS users, within CBP, in November 2011. A further demonstration of this technology fix is planned for an additional 12 TECS users across DHS components in March 2012. Lastly, with regard to IOIL Incident Log (Immigration Operations), TECS Modernization has scheduled a planned implementation of functionality to remove the use of supervisor SSNs from approval functions, affecting 8,000 users, by March 2013.

Completion Date: March 31, 2013

With regard to the sensitivity of the draft report, CBP has not identified information within the report requiring restricted public access. Enclosed for your consideration are CBP's technical comments.

CBP acknowledges its continuing challenge to embed a culture of privacy within all of its employees. CBP also recognizes that this challenge and the safeguarding of its vast information holdings are only successfully met through a shared understanding and practice of all employees, from the Commissioner on down. Once again, thank you for the opportunity to comment on the draft report.

We look forward to working with you on future reviews. If you have any questions, please have a member of your staff contact Kathryn Dapkins, Audit Liaison, Office of Internal Affairs at (202) 344-2102.

Sincerely,

FOR:

James F. Tomsheck
Assistant Commissioner
Office of Internal Affairs

Enclosures

Appendix C
Legislation, Memoranda, Directives, and Guidance Related to CBP Privacy Stewardship Audit

LEGISLATION

Privacy Act of 1974, as amended, 5 U.S.C. § 552a.
http://www.gpo.gov/fdsys/pkg/USCODE-2010-title5/pdf/USCODE-2010-title5-partI-chap5-subchapII-sec552a.pdf

E-Government Act of 2002, Public Law 107-347, 116 Stat. 2899.
http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

Federal Information Security Management Act of 2002, 44 U.S.C. § 3541, et seq.
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, 121 Stat. 266, 360.
http://www.nctc.gov/docs/ir-of-the-9-11-comm-act-of-2007.pdf

The Security and Accountability For Every Port Act of 2006, Public Law 109-347, 120 Stat. 1884, 1924.
http://www.gpo.gov/fdsys/pkg/PLAW-109publ347/pdf/PLAW-109publ347.pdf

Homeland Security Act of 2002, as amended, Public Law 107-296, 116 Stat. 2135, 2179 (2002).
http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf

OMB MEMORANDA

OMB M-07-16: *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007). http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

DIRECTIVES AND GUIDANCE

DHS Memorandum: *Designation of Component Privacy Officers* (June 5, 2009). (No External Link Available)

DHS Management Directive Number 0470.2: *Privacy Act Compliance* (October 6, 2005).
http://www.dhs.gov/xlibrary/assets/foia/mgmt-directive-0470-2-privacy-act-compliance.pdf

Privacy Policy Guidance Memorandum Number 2008-01: *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (December 29, 2008).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

Privacy Policy Guidance Memorandum Number 2008-02: *DHS Policy Regarding Privacy Impact Assessments* (December 30, 2008). http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf

Privacy Policy Guidance Memorandum Number 2007-01: *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons* (January 7, 2009).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

Privacy Policy Guidance Memorandum Number 2007-02: *Use of Social Security Numbers at the Department of Homeland Security* (June 4, 2007). http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-2.pdf

DHS Privacy Office: *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security* (October 6, 2011). http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf

DHS Privacy Office: *Privacy Incident Handling Guidance* (September 10, 2007).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf

DHS Privacy Office: *Privacy Technology Implementation Guide* (August 16, 2007).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_ptig.pdf

DHS Privacy Office: *Privacy Impact Assessments: The Privacy Office Official Guidance* (June 2010).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf

DHS Privacy Office: *System of Records Notices Official Guidance* (April 2008).
http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_sorn.pdf

Office of Personnel Management Memorandum: *Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft* (June 18, 2007).
http://www.cio.gov/Documents/Guidance_on_Protecting_Fed_Emp_SSNs.pdf

Appendix C
Legislation, Memoranda, Directives, and Guidance Related to CBP Privacy Stewardship Audit

CBP DOCUMENTS

Memorandum from the Acting Commissioner, U.S. Customs and Border Protection, to Deputy Secretary, Department of Homeland Security (July 28, 2009). (No External Link Available)

CBP Records Disposition Schedule (2001). (No External Link Available)

Office of Information Technology: *Information Systems Security Policies and Procedures Handbook Version 2.0,* HB1400-05D (July 27, 2009). (No External Link Available)

Appendix D
Component-Level Privacy Officer Designation and Duties

COMPONENTS TO DESIGNATE PRIVACY OFFICERS

- U.S. Customs and Border Protection
- Federal Emergency Management Agency
- National Protection and Programs Directorate
- Office of Intelligence and Analysis
- Science and Technology Directorate
- Transportation Security Administration
- U.S. Citizenship and Immigration Services
- U.S. Coast Guard
- U.S. Immigration and Customs Enforcement
- U.S. Secret Service

COMPONENT PRIVACY OFFICER DUTIES

Communicate the component privacy initiatives, both internally and externally.

Monitor component's compliance with all Federal privacy laws and regulations; implement corrective, remedial, and preventative actions; and notify the DHS Privacy Office of privacy issues or noncompliance when necessary.

Provide privacy information to the DHS Privacy Office for the quarterly *Federal Information Security Management Act* reporting, Section 803 of the *Implementing Recommendations of the 9/11 Commission Act* reporting, the DHS Privacy Office Annual Report, and other reporting requirements, as needed.

Serve as the point of contact to handle privacy incident response responsibilities as defined in the *Privacy Incident Handling Guidance*.

Assist program managers and system of records owners in drafting and reviewing Privacy Threshold Assessments, Privacy Impact Assessments, and System of Records Notices, as well as any associated privacy compliance documentation.

Implement and monitor privacy training for employees and contractors.

Source: DHS Memorandum, *Designation of Component Privacy Officers*, June 5, 2009.

Appendix E
CBP Culture of Privacy Survey

We developed a privacy questionnaire with involvement of the CBP Privacy Officer. In May 2011, we e-mailed CBP employees a hyperlink to a secure site to complete an online culture of privacy survey. Survey participation was voluntary, confidential, and accessible only by OIG.

The purposes of the survey were to obtain employees' responses to three questions regarding privacy risks, integrating privacy in daily operations, and challenges in CBP privacy stewardship, as well as to assess their privacy knowledge based on the criteria in appendix C.

A total of 7,727 respondents completed the CBP Culture of Privacy Survey. The completed survey response rate was 13.1 percent (7,727 of 58,844). The following figure provides the levels of job responsibility, locations, and lengths of service of respondents who completed the survey.

DEMOGRAPHICS (n 7,727 Survey Respondents)
Level of Job Responsibility
Entry-level Employees (16.6%)
Mid- to High-level (Non-manager) Employees (60.2%)
Supervisors/First-Line Managers (18.9%)
Executive/Senior Managers (4.3%)
Location
Office of the Commissioner and Mission Support Offices (19.2%)
Office of Field Operations (48.6%)
Office of Border Patrol (29.5%)
Office of Air and Marine (2.7%)
Length of Service
Less than 3 months (0.8%)
3–12 months (4.2%)
1–3 years (16.6%)
More than 3 years (78.4%)

Figure 7. Demographics of Survey Respondents

We received a total of 7,229 individual comments and suggestions for improvements from the survey respondents. We categorized these comments by six subjects: Culture of Privacy, Privacy Stewardship, Data Governance, Administrative Safeguards, Technical Safeguards, and Physical Safeguards. The percentages of recommended improvements in each of the six categories are indicated in the pie chart, illustrated in figure 8.

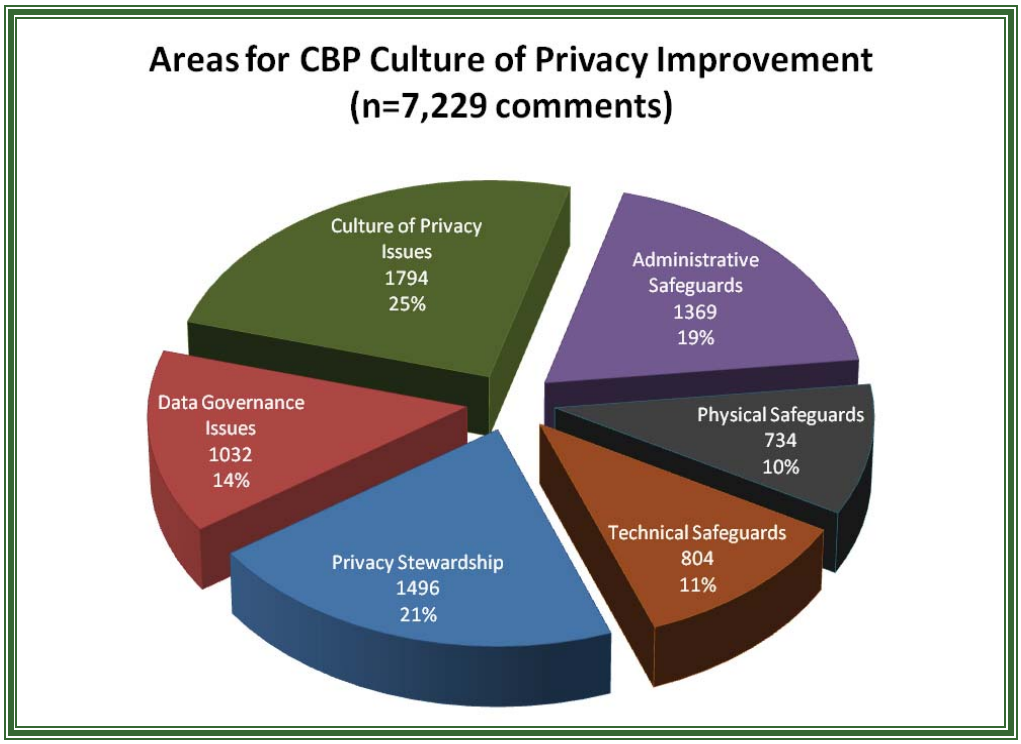

Figure 8. Areas for CBP Culture of Privacy Improvement

Comments on **Culture of Privacy**, 1,794 (25%), recommended improvements by executive managers, program operations managers, and employees in understanding and applying their privacy responsibilities, such as the following:

- A shared strategic vision on privacy matters throughout the organization (657);
- Advancement of employee privacy protections, such as discontinuing the use of Social Security numbers (579); and
- Mitigation of job-specific risks unique to employee work environments (558).

Comments on **Privacy Stewardship**, 1,496 (21%), identified the need for CBP to advance privacy as an operational priority. Respondents recommended improvements, such as the following:

- Managerial and supervisory roles in encouraging the advancement of privacy through their example and ensuring uniform accountability (798);
- Accessibility of consistent privacy guidance and policies with defined privacy goals and guidelines to achieve them (437);
- Privacy protections on the job through the use of reminders (230); and
- CBP Privacy Officer's role in privacy (31).

Comments on **Data Governance**, 1,032 (14%), involved the consistent and proper management of data during collection, use, storage, and disposition. Respondents recommended improvements, such as the following:

- Records management guidance on retention and disposition of PII (375);
- Guidance explicitly limiting distribution of public and employee PII to individuals with a need-to-know disclosure (257);
- Data quality and integrity (239); and
- Guidance and practices regarding whether information should be shared (161).

Comments on **Administrative, Physical, and Technical Safeguards**, 2,907 (40%), are discussed in a separate section of the report. Of all safeguards recommended, 743 (25%) comments focused on improving privacy training, such as the following:

- Increased frequency (346);
- Expanded delivery options (232);
- Incorporated privacy applications, using on-the-job and real-world examples that relate to the different programs and operations at CBP (85);
- Added specialized privacy training for particular groups, such as new employees, supervisors, and executive managers (49); and
- Simplified presentations and concepts for easier application to daily operations (31).

Appendix F
CBP Privacy Compliance Status

OMB M-07-16 requires agencies to review their holdings of all PII and ensure that they are accurate, relevant, timely, and complete. DHS privacy policy guidance requires a **privacy threshold analysis** to be conducted every three years when significantly changing existing systems, or when proposing new systems. The *E-Government Act of 2002* requires a **privacy impact assessment** to be conducted for all new or substantially changed information systems that collect, maintain, or disseminate PII to ensure that privacy protections are incorporated during the development and operation of systems and programs that affect PII. The *Privacy Act of 1974* requires a **system of record notice** to inform the public about what PII is being collected, why it is being collected, how long it is being retained, and how it will be used, shared, accessed, and corrected. The status of privacy compliance documentation could affect how CBP should address privacy or trigger further review concerning the need to update privacy threshold analysis, privacy impact assessments, or system of record notices on the underlying systems.

Figure 9 provides the privacy compliance status for 95 systems. The figure shows the date of documentation for 47 systems or programs that the CBP Privacy Officer identified as his inventory of PII as of July 2011. Of the 47 systems or programs, 16 do not require a privacy impact assessment and three do not require a system of records notice. In addition, we compared several sources, including CBP's information reported in Trusted Agent's inventory, CBP/Information Technology Intranet website, DHS Privacy Office's public website, and interviews with CBP personnel, and identified 48 potential systems or programs during the course of the audit. The legend for our determinations is:

Completed	Privacy threshold analysis, privacy impact assessment, or system of records notice on file
Need	DHS Privacy Office/CBP agree that privacy impact assessment and/or system of records notice are/is required
None	Privacy threshold analysis was unavailable; CBP needs to make a determination
Not Applicable	Either a system of records notice or privacy impact assessment does not apply to information technology systems in CBP's inventory
Other	May be part of, but not fully addressed by, CBP's published privacy impact assessments or system of records notices
Undetermined	May affect privacy, but does not have a privacy threshold analysis. Therefore, we cannot determine whether the system requires a privacy impact assessment or system of records notice
Out of Date	Privacy threshold analysis has expired date

Name	Types of Personally Identifiable Information	Privacy Threshold Analysis	Privacy Impact Assessment	System Of Records Notice
Automated Commercial Environment (ACE)/Automated Commercial System (ACS) and Associated Applications				
Automated Commercial Environment (ACE)	Broker, Cargo, Carrier, Importer	Completed Jun 15, 2006	Completed Jul 14, 2006	Completed Jan 19, 2006
Automated Commercial System (ACS)	Broker, Cargo, Carrier, Importer	Completed Nov 9, 2007	Completed Dec 2, 2008	Completed Dec 19, 2008

Appendix F
CBP Privacy Compliance Status

Name	Types of Personally Identifiable Information	Privacy Threshold Analysis	Privacy Impact Assessment	System Of Records Notice
Automated Export System (AES)	Broker, Cargo, Carrier, Importer	Completed Nov 9, 2007	Need	Need
Secure Freight Initiative International Container Security (SFI/ICS)[2]	Cargo	None	Other	Other
Automated Targeting System (ATS) and Associated Modules				
Automated Targeting System (ATS)	Traveler, Conveyance, Cargo	Completed Mar 28, 2008	Completed Dec 2, 2008	Completed Aug 6, 2007
Automated Targeting System Inbound (ATS-N)[2]	Traveler, Conveyance, Cargo	None	Other	Other
Automated Targeting System Intelligence and Operations Framework System (IOFS)	Traveler, Conveyance, Cargo	Undetermined	Undetermined	Undetermined
Automated Targeting System Land (ATS-L)[2]	Traveler, Conveyance, Cargo	None	Other	Other
Automated Targeting System Outbound (ATS-AT)[2]	Traveler, Conveyance, Cargo	None	Other	Other
Automated Targeting System Passenger (ATS-P)[2]	Traveler, Conveyance	None	Other	Other
Automated Targeting System TAP (Trend Analysis and Analytical Selectivity Program)[2]	Traveler, Conveyance, Cargo	None	Other	Other
E3: Next Generation of ENFORCE	Traveler	Completed Oct 26, 2007	Need	Completed Mar 20, 2006
Global Enrollment System / Western Hemisphere Travel Initiative and Associated Applications				
Global Enrollment System (GES)	Traveler, Passenger	Completed Jul 27, 2006	Completed Apr 20, 2006	Completed Apr 21, 2006
Global Entry	Traveler, Passenger	Completed Jul 14, 2006	Completed Apr 20, 2006	Completed Apr 21, 2006
Global Online Enrollment System (GOES)[2]	Traveler, Passenger	None	Other	Other
Western Hemisphere Travel Initiative (WHTI)	Traveler	Completed Apr 18, 2007	Completed Mar 24, 2008	Completed Dec 19, 2008
Decal and Transponder Online Procurement System (DTOPS)	Conveyance	Completed Oct 14, 2009	Need	Completed Apr 21, 2006
Free and Secure Trade (FAST)[1, 2]	Cargo	None	Other	Other
Customs-Trade Partnership Against Terrorism (CTPAT)	Broker, Cargo, Carrier, Importer	Completed Oct 22, 2009	Need	Need
TECS and Associated Functions or Resides on TECS Platform				

Appendix F
CBP Privacy Compliance Status

Name	Types of Personally Identifiable Information	Privacy Threshold Analysis	Privacy Impact Assessment	System Of Records Notice
TECS	Traveler, Employee	Completed Jan 2, 2008	Completed Dec 22, 2010	Completed Dec 19, 2008
TECS Modernization	Traveler, Employee	Completed Oct 4, 2007	Completed Dec 22, 2010	Completed Dec 19, 2008
Advanced Passenger Information System (APIS)[2]	Passenger, Crew	None	Other	Other
Advanced Passenger Information System (APIS) Pre-Departure[2]	Passenger, Crew	None	Other	Other
Electronic Advanced Passenger Information System (eAPIS)[2]	Passenger, Crew	None	Other	Other
Integrated Advanced Passenger Information System (IAPIS)[2]	Passenger, Crew	None	Other	Other
Border Security Deployment (BSD)	Employee, Contractor, Traveler	Completed Apr 7, 2010	Need	Completed Dec 19, 2008
CBP Vetting[2]	Traveler	None	Other	Other
DataShare Project Immigrant and Non-immigrant Visas[2]	Traveler	None	Other	Other
License Plate Reader (LPR)[1]	Traveler	Completed Sep 8, 2009	Completed Jan 2, 2008	Completed Dec 19, 2009
NIDPS External Interfaces[1]	Traveler, Passenger	Undetermined	Undetermined	Undetermined
Outlying Area Reporting Station (OARS)	Traveler	Undetermined	Undetermined	Undetermined
Pedestrian Primary Processing[1, 2]	Traveler, Employee	None	Other	Other
Pleasure Boat Reporting System (PBRS)[2]	Traveler, Conveyance	None	Other	Other
Portable Automated Lookout System (PALS)[1, 2]	Traveler	None	Other	Other
Primary Lookout Override (PLOR)[1, 2]	Traveler, Passenger	None	Other	Other
Regional Movement Alert System (RMAS)	Passenger, Crew	Undetermined	Undetermined	Undetermined
Regulatory Audit Management Information System (RAMIS)	Broker	Completed Aug 4, 2008	Not Applicable	Completed Dec 19, 2008

Appendix F
CBP Privacy Compliance Status

Name	Types of Personally Identifiable Information	Privacy Threshold Analysis	Privacy Impact Assessment	System Of Records Notice
TECS – TECS Case Management[1, 2]	General public involved in specific cases	None	Other	Other
TECS – Inspection Operations – Secondary Processing[1, 2]	Traveler, Passenger	None	Other	Other
TECS – TECS/NIIS[1, 2]	Traveler, Passenger	None	Other	Other
TECS – TECS Reporting[1, 2]	Traveler, Employee	None	Other	Other
Traveler Primary Arrival Client (TPAC)[1, 2]	Passenger, Crew	Completed Feb 24, 2010	Other	Other
Vehicle Primary Processing[1, 2]	Traveler, Employee	None	Other	Other
Data sets or feeds supplied by other Government agencies for use by CBP, covered by CBP information sharing access agreement, and reside within the boundary of a CBP system				
Currency or Monetary Instruments Report (CMIR)[2]	Traveler	None	Other	Other
Customs Automated Maintenance Inventory Tracking System (CAMITS)	Employee, Contractor	Completed Jan 30, 2009	Not Applicable	Completed Dec 29, 2006
Interstate Identification Index (III)[2]	Traveler	None	Other	Other
National Crime Information Center (NCIC)[2]	Traveler, Passenger	None	Other	Other
National Law Enforcement Telecommunications System (NLETS)	Traveler, Passenger	Undetermined	Undetermined	Undetermined
Private Aircraft Enforcement System (PAES)[1, 2]	Passenger	None	Other	Other
Security Filing[2]	Broker, Cargo, Importer	None	Other	Other
U.S. Passport Load from Department of State[2]	Traveler, Passenger	None	Other	Other
UNCATEGORIZED: May be subsystem or module that is a major subdivision or component of an information system; tools, application software, or specialized functionality to the hosted information system; or, infrastructure, data set or feed, interface, or service within the boundary of a system. These systems may include administrative, human resources, or financial systems.				
10-Print Pilot Initiative[1]	Passenger, Crew	Undetermined	Undetermined	Undetermined
Active Directory/Exchange (ADEX)	Employee, Contractor	Completed Feb 24, 2010	Completed Jan 14, 2009	Completed Sep 29, 2009

Appendix F
CBP Privacy Compliance Status

Name	Types of Personally Identifiable Information	Privacy Threshold Analysis	Privacy Impact Assessment	System Of Records Notice
Air and Marine Operations Surveillance System (AMOSS)	Traveler, Cargo	Completed Jul 28, 2009	Need	Not Applicable
Analytical Framework for Intelligence (AFI)	Traveler, Broker, Cargo, Carrier, Importer	Completed Jan 9, 2009	Need	Need
Audit and Review Tracking System (ARTS)[1]	Employee	Undetermined	Undetermined	Undetermined
Blackberry Enterprise Server and Wireless Handheld Devices (BES WHD)	Employee, Contractor	Completed Aug 10, 2009	Completed Jan 14, 2009	Completed May 15, 2008
Border Patrol Enforcement Tracking System (BPETS)	Employee, Contractor, Traveler	Completed Jul 28, 2006	Need	Completed Dec 19, 2008
Border Patrol Enforcement Tracking System 2 (BPETS 2)	Employee, Contractor, Traveler	Completed Jan 29, 2009	Need	Completed Mar 20, 2006
Cargo Enforcement Reporting and Tracking System (CERTS)[1]	Broker, Cargo, Carrier, Importer	Undetermined	Undetermined	Undetermined
Computerized Aircraft Reporting Materiel Control (CARMAC)	Employee, Contractor	Completed Mar 24, 2010	Not Applicable	Need
CBP Application Integration Project (CAIP)	Employee, Contractor	Completed Jan 21, 2009	Not Applicable	Completed May 15, 2008
CBP Automated Pre-Employment System (CAPES)[1]	Employee	Undetermined	Undetermined	Undetermined
CBP Automated Travel System (CATS)	Employee	Undetermined	Undetermined	Undetermined
CBP Complaint Management System (CMS)	Traveler	Undetermined	Undetermined	Undetermined
CBP Overtime Schedule System (COSS)	Employee	Undetermined	Undetermined	Undetermined
CEAR[1]	Employee, Contractor	Undetermined	Undetermined	Undetermined
Combined Automated Operations System (CAOS)	Employee, Contractor	Completed Oct 23, 2006	Not Applicable	Completed Oct 28, 2008
Dedicated Commuter Lane (DCL)[1]	Traveler	Undetermined	Undetermined	Undetermined
Enterprise Data Warehouse (EDW)	Employee, Contractor, Traveler, Cargo	Completed Jan 23, 2007	Need	Need
Enterprise Geospatial Information Services (eGIS)	Traveler	Completed Nov 1, 2007	Not Applicable	Completed May 15, 2008

Appendix F
CBP Privacy Compliance Status

Name	Types of Personally Identifiable Information	Privacy Threshold Analysis	Privacy Impact Assessment	System Of Records Notice
Enterprise Service Bus (ESB)	Employee, Contractor	Completed Aug 5, 2008	Need	Need
Enterprise Management Information System –- Enterprise Data Warehouse (EMIS EDW)	Employee, Contractor, Traveler, Cargo	Completed Mar 24, 2010	Need	Need
Electronic System for Travel Authorization (ESTA)	Traveler	Completed Nov 10, 2010	Completed Jul 18, 2011	Completed Jun 10, 2008
Firearms, Armor, and Credentials Tracking System (FACTS)	Employee	Completed Apr 3, 2008	Not Applicable	Completed Oct 23, 2008
I-94 Form, Non-Immigrant Information Data Processing System (NIDPS) formerly NIIS[2]	Traveler, Passenger	None	Other	Other
I-94 Secondary Processing Project[2]	Traveler, Passenger	None	Other	Other
Intellectual Property Rights Search (IPRS)[1]	General public	Undetermined	Undetermined	Undetermined
Intelligent Computer Assisted Detection (ICAD)	Traveler, Passenger	Completed Dec 2, 2009	Need	Need
Joint Integrity Case Management System (JICMS)	Employee, Contractor	Completed Feb 1, 2010	Need	Completed Nov 14, 2008
National Finance Center Field LAN System	Employee, Contractor	Completed Jan 7, 2009	Not Applicable	Completed Oct 23, 2008
National Data Center Administrative Applications (NDC Administrative Apps)	Employee, Contractor	Completed Oct 23, 2006	Not Applicable	Completed Mar 5, 2007
National Data Center Financial Applications (NDC Financial Apps)	Employee	Completed Jan 23, 2009	Not Applicable	Completed Oct 23, 2008
National Data Center Mainframe Infrastructure System	Employee	Completed Apr 21, 2008	Not Applicable	Completed May 15, 2008
Non-Intrusive Inspection (NII) Systems Program	Cargo, Carrier	Completed Sep 5, 2007	Need	Not Applicable
National Targeting Center LAN System (NTC LAN)	Employee, Contractor	Completed Dec 7, 2006	Not Applicable	Completed Dec 29, 2006
OpSTAR	Employee, Contractor	Completed Oct 3, 2008	Not Applicable	Completed May 15, 2008
Quality and Uniformity Information Control System (QUICS)	Broker, Cargo, Carrier, Importer	Undetermined	Undetermined	Undetermined
Remedy Incident Reporting (Remedy)	Employee, Contractor	Completed Jan 29, 2009	Not Applicable	Completed Sep 29, 2009

Appendix F
CBP Privacy Compliance Status

Name	Types of Personally Identifiable Information	Privacy Threshold Analysis	Privacy Impact Assessment	System Of Records Notice
Systems, Applications, and Products (SAP)	Employee, Contractor	Completed Mar 19, 2009	Not Applicable	Completed Dec 29, 2006
Secure Border Initiative-net (SBInet)	Biometrics	Completed Dec 2, 2009	Completed Jul 20, 2007	Not Applicable
SBInet Northern Border	Biometrics	Completed Jul 6, 2011	Need	Need
SBInet Southern Border	Biometrics	Completed Jul 6, 2011	Need	Need
Seized Asset and Case Tracking System (SEACATS)	Broker, Cargo, Carrier, Importer	Completed Nov 5, 2007	Need	Completed Dec 19, 2008
Virtual Learning Center (VLC)	Employee, Contractor	Completed Sep 8, 2009	Not Applicable	Completed May 8, 2006

Figure 9. CBP Privacy Compliance Status

[1] Listed on CBP Intranet, Office of Information Technology/program office pages, but not in Trusted Agent.
[2] Some privacy risks may be mitigated by information technology controls as described by pertinent system security plans or other information technology documentation.

Appendix G
Inconsistencies Between Records Retention Schedules Published in System of Records Notices and Internal Guidance

According to the Privacy Act, information in the published system of records notices must accurately describe how Government employees handle the public's PII. We reviewed 26 different types of records described in CBP's system of records notices for 34 systems. Figure 10 lists the 26 types of records that are described in the system of records notices.

Types of Records	
Aircraft Manifest	Arrival-Departure Record for Nonimmigrant Visitors with a Visa for the U.S.
Land Vehicle Manifest	Trusted Traveler Program Information
Sea Vessel Manifest	Travel Document Information
Postal Declaration	Foreign National Arrival-Departure Information in Electronic and Paper Format
Carrier, Broker, Importer/Exporter Account Information	Records Related to a Law Enforcement Action
Importer Security Filing	Regulatory Audit Files
Shipper's Information	Law Enforcement Records, including Expired Statutes of Limitation
Passenger Name Record	Carrier Records
Border Crossing Information of U.S. Citizens and Lawful Permanent Residents	Broker Files
Border Crossing Information of Nonimmigrant Visitors	Cartmen and Lightermen Files
Recordings with Security Incidents	Warehouse Proprietor Records
Recordings with Actions Taken by CBP	Driver Records
Foreign National Information via Visa Waiver Program	Information on Proprietor Bonded Warehouse Operators and Employees

Figure 10. Types of Records Described in CBP's Published System of Records Notices

Records retention and disposal schedules are documents that identify an organization's records and provide instructions on how long to retain or maintain records and when to dispose of records. We compared the published schedules in the system of records notices with CBP's internal guidance. Using guidance issued internally by CBP, employees are not retaining PII for the same periods of time as published for the public in the system of records notices. Figure 11 indicates the number of records identified in the system of records notices by type of inconsistency.

Type of Inconsistency	# Inaccurate Records Scheduled	Percentage
Records disposed of before the time published in the system of records notices	**7**	**26.9%**
Records held longer than the time published in the system of records notices	**13**	**50.0%**
Retention and disposal of records not addressed by internal guidance	**6**	**23.1%**
Total # record schedules described in the system of records notices	**26**	**100%**

Figure 11. Inconsistencies in CBP's Personally Identifiable Information Records Retention and Disposal Schedules

Appendix H
DHS Fair Information Practice Principles at Work

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

The Fair Information Practice Principles at Work

DHS issued Privacy Policy Guidance Memorandum 2008-01 on December 29, 2008 memorializing the Fair Information Practice Principles (FIPPs) as the foundational principles for privacy policy and implementation at DHS. The eight FIPPs form the basis of the Department's privacy compliance policies and procedures governing the use of personally identifiable information (PII). The FIPPs are embedded into DHS privacy sensitive systems, programs, and information sharing arrangements and are derived from the Privacy Act and other federal and international privacy guidelines. This document provides some typical examples of how the DHS Privacy Office oversees implementation of the FIPPs in the Department.

Transparency

DHS employs several means to provide transparency to the public of its activities and DHS privacy protections. DHS provides public notice of the collection, use, dissemination, and maintenance of PII through various mechanisms including: direct notice (commonly referred to as a Privacy Act e (3) statement) on forms used to collect information from individuals,; signage at U.S. ports of entry; and publication of privacy compliance documentation such as Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs). More broadly, DHS implements transparency by making its PIAs, SORNs, guidance, and other reports, including congressionally-mandated reports, available on the DHS Privacy Office website located at http://www.dhs.gov/privacy. In some instances, law enforcement or national security concerns prevent public disclosure of specific details of systems and programs. In these defined cases, DHS notifies the public of the exemptions for relevant systems. Even for these exempted systems, however, DHS reviews access requests on a case-by-case basis.

Individual Participation

DHS and its components have varied missions, including benefits administration, grants administration, border management, transportation security, cyber security, law enforcement, and national security. When programs carried out in pursuit of these missions require the collection of PII, DHS seeks to collect PII directly from individuals. If an individual believes a benefit was denied or some type of Departmental action (e.g., a referral to secondary screening) was taken as a result of an error in his information, that individual may, regardless of citizenship, seek access to, and, as appropriate, correct his information through the Freedom of Information Act (FOIA)/Privacy Act process. Furthermore, DHS developed the DHS Traveler Redress Inquiry Program (DHS TRIP) to be a single point of contact to handle questions and concerns about travel screening. An individual has the additional option of submitting a request for correction directly with the DHS Chief Privacy Officer. Recognizing that certain DHS functions are law enforcement or national security sensitive, DHS will not always collect information directly from the individual or permit access to and/or correction of records through the FOIA/Privacy Act process. In these cases, the Department provides notice through the relevant system Privacy Act exemption(s), and through response to related inquiries.

Purpose Specification

DHS articulates the legal authority that permits the collection of PII as well as the purpose or purposes for which the PII is intended to be used in its PIAs and SORNs. As part of the privacy compliance process, a program must be able to articulate the need for a particular collection of information with an appropriate legal authority and purpose justification.

Website: www.dhs.gov/privacy Email: privacy@dhs.gov Phone: 703-235-0780

Appendix H
DHS Fair Information Practice Principles at Work

Data Minimization

DHS seeks to minimize its collection of PII through its privacy compliance processes in two ways. First, the DHS Privacy Office works with the Office of the Chief Information Officer on the Paperwork Reduction Act process that seeks to minimize the collection of information, including PII from the public. Second, PIAs and SORNs require that data elements being collected are both relevant and necessary for the stated purpose of the system. DHS places a special emphasis on reducing the use of Social Security numbers (SSNs). DHS does not collect SSNs unless there is a valid authority for their collection.

Use Limitation

DHS limits its uses of PII to those that are permissible under law, and articulated in published PIAs and SORNs. Uses may include sharing both inside and outside of DHS. Within the Department, use of PII is limited to personnel who have an authorized need-to-know for the information. For external sharing, these uses are legally defined "routine uses," and must be compatible with the original collection and purpose specification. Absent a statutory requirement to disclose specific information, such routine use sharing decisions are made following a case-by-case review by the DHS Privacy Office to ensure a request meets the requirements. Sharing PII with external entities is done pursuant to routine uses articulated in published SORNs and may also be authorized by a written information sharing agreement, such as a Memorandum of Understanding, between the Department and the receiving agency.

Data Quality and Integrity

To ensure data quality, DHS collects information directly from the individual where practicable, especially in benefit administration functions. Recognizing data errors occur, DHS has implemented redress mechanisms that enable individuals to seek access and correction of their information through the FOIA/Privacy Act process, as described above. Travelers who experience difficulties may also seek redress through DHS TRIP.

Security

Since privacy and security are complementary, DHS Privacy Office works closely with the Office of the Chief Information Officer and the Chief Information Security Officer to ensure that security controls are put in place in IT systems that are commensurate with the sensitivity of the information they hold. Privacy requirements are built into the DHS Sensitive Systems Security Policy to safeguard PII from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction. By law, such systems must be certified as meeting relevant security standards. System and program managers are required to complete a Privacy Threshold Analysis, as well as a PIA and SORN, if applicable, before an IT system becomes operational.

Accountability and Auditing

DHS' privacy protections are subject to oversight by its Chief Privacy Officer and Inspector General as well as by the Government Accountability Office and the U.S. Congress. In addition to these oversight mechanisms, component privacy officers, system owners, and program managers implement accountability in their systems and programs through activities such as periodic review of audit logs to ensure that uses of PII are consistent with the purposes articulated for the collection of that information, as required by the Privacy Act. Further, as public documents, PIAs and SORNs not only demonstrate transparency but also serve as means by which the public can hold the Department accountable for its collection, use, and sharing of PII.

June 2011

Website: www.dhs.gov/privacy Email: privacy@dhs.gov Phone: 703-235-0780

Appendix I
Major Contributors to this Report

Marj Leaming, Director
Eun Suk Lee, Lead Privacy Auditor
Kevin Mullinix, Program Analyst
Steven Tseng, Management and Program Assistant
Ernest Bender, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Commissioner of CBP
DHS Privacy Office
CBP Audit Liaison Office
CBP Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, or e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsoig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to Department of Homeland Security programs and operations:

- Call our Hotline at 1-800-323-8603

- Fax the complaint directly to us at (202)254-4292

- E-mail us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigation - Hotline,
  245 Murray Drive SW, Building 410
  Washington, DC 20528

The OIG seeks to protect the identity of each writer and caller.